North Carolina
Statewide Technical Architecture

Security Domain

© 2005 State of North Carolina
Office of the State Chief Information Officer
Enterprise Technology Strategies
PO Box 17209
Raleigh, North Carolina 27699-7209
http://www.ncsta.gov
ets@ncmail.net

Table of Contents

1. Principles:

1.1. Implementation of proven security policies, procedures, and controls greatly improves the security posture of an organization.

Rationale:

- Security policies are management directives for directing, governing, and regulating an organization's security requirements. Security procedures and controls detail the processes required to implement the types and levels of protection necessary.
- Successful security efforts depend on management and staff commitment to the protection of resources.
- Security is only as strong as its weakest link. A lack of alignment opens opportunities for exploiting differences in commitment to and implementation of security processes and solutions.

1.2. Security controls for State assets must be commensurate with their value and sufficient to contain risks to an acceptable level.

Rationale:

- Security is a business necessity with associated costs. Security expenditures should be a balance between cost and risk.
- Qualitative or quantitative analysis techniques can be utilized to determine the proper amount of money to budget to protect assets.
- Requirements for security vary depending on the information system, connection to other systems, sensitivity of data, and probability of harm.
- The state has a responsibility to ensure its data meets regulatory (e.g. HIPAA) and public safety requirements. These requirements must be considered when planning security levels.

1.3. Comprehensive security programs are essential. Program operation should occur within either an Agency or Statewide Security Office.

Rationale:

- Recent policy-based internal security assessments have shown the need to establish a security program or security office. Without a coordinated and on-going security initiative in place, the ability to adequately secure the State's IT assets over time becomes increasingly less possible.
- Security programs should focus on accomplishing both the strategic and tactical aspects of security which include identifying and prioritizing security related needs, providing Agency CIOs with professional guidance on the best ways to better secure an organization, developing and implementing a security training program for both IT and end users, and performing incident response activities.

1.4. Focusing on assuring data confidentiality, availability, integrity, and accountability ensures that the State's business objectives and security policies are satisfied[1].

Rationale:

- The availability of data is essential in ensuring security. If data is inaccessible by authorized personnel important decisions or processes are delayed. Furthermore, confidence is easily lost when data cannot be accessed.
- It is critical to ensure that data or systems have not been altered in an unauthorized manner. Corrupted data jeopardizes all business functions and requires that recovery processes be invoked when discovered.
- Data confidentiality is more important than ever. Only authorized entities can be allowed to access data. Agencies must comply with privacy laws; failures in this area could result in fines or the need to notify the citizenry of data exposure.

1.5. Classifying information as either Public or Confidential helps to ensure compliance with legal and regulatory requirements and protects the privacy of citizens, businesses, and employees.

Rationale:

- By law, the general public has the right to request access to government information. If the information has been classified as Public, then the information can be made available according to established procedures. Access to Confidential information must be authorized on a strict "need to know" basis, in conformance with legal requirements for allowable access.
- Confidentiality is to be determined in accordance with NCGS Chapter 132 - Public Records Law and all other applicable legal and regulatory requirements.
- Occurrences of identity theft continue to rise. Public and confidential information must be secured and only revealed to requestors according to approved procedures.
- Government has a responsibility to perform its duties as required by law; however these duties must be performed in a manner that ensures privacy.

1.6. Security is an integral part of all stages of the Software Development Life Cycle (SDLC)[2].

Rationale:

- Security must be planned from the very beginning of the SDLC (i.e. Initiation Phase); otherwise securing the system is much more costly and inefficient.
- Systems already in production (Maintenance Phase) must also be secured.
- Even when systems are being retired (Disposal Phase) the proper actions must be taken to ensure the system is decommissioned securely
- Designing for security from inception to implementation is significantly less costly than post-implementation attempts to retrofit security into applications.

[1] NIST Special Publication 800-33 – Underlying Technical Models for Information Security.

[2] NIST Special Publication 800-27 – Engineering Principles for Information Technology Security.

- Refer to the Application Domain for further information regarding the development of secure applications.

1.7. Utilizing defense-in-depth[3] and layered security approaches protects the State's information assets.

Rationale:

- The use of layered security controls across all aspects of network and application better protects resources from various security threats and vulnerabilities, thereby reducing the overall risk of a potential security incident.
- The use of layered security controls and mechanisms better protects the asset if security controls are circumvented.
- Protection of a resource is best accomplished by placing controls as close to the resource as possible. Additional layers of security help to protect the resource in the event that the primary means of protection fails for any reason.
- Due to the diverse needs of the State, a single security perimeter that protects the entire network and all related systems was not feasible. For this reason, a Security Zoning model has been developed, which is consistent with a layered security approach.
- Refer to the Security Zoning Technical Topic for more information.

1.8. A security architecture that leverages an integrated set of enterprise services permits state agencies to focus on the business goals rather than on the implementation of security.

Rationale:

- Utilize the State's infrastructure security services.
- Integration of security services will enable interoperability and provide flexibility in conducting electronic business across and beyond the enterprise.
- Integration will reduce the costs of protecting the state's resources.
- Integration will increase the reliability of security solutions.

1.9. Security risk assessments are effective in identifying vulnerabilities; once identified, actions can be taken to mitigate unacceptable levels of risk.

Rationale:

- A security risk assessment should be performed for all new and ongoing business systems. To determine the appropriate security requirements, business units should assess the value of system assets, risk exposure to those assets, and evaluate the mitigation measures and costs of protecting those systems.
- Understanding the value of assets and associated risks is essential to determining the level of security required.
- Security requirements should be included when designing or purchasing new applications.
- Security requirements should utilize enterprise security resources where available.

[3] NIST Special Publication 800-27 – Engineering Principles for Information Technology Security.

1.10. Security solutions that are based and built on proven open industry standards facilitate intra and inter-application integration.

Rationale:

- Proprietary security services that have not been publicly vetted cannot be trusted and therefore must not be used. This is especially true in the area of cryptography (e.g. encryption and Public Key Infrastructure).
- Statewide security services will often be provided as infrastructure services. In order to take advantage of these services, application security must be designed to utilize open standards. A clear migration path should be defined for products that are not capable of integrating with the infrastructure security services.
- Use of open industry standards facilitates intra and inter-application integration that has been established via an overall security architecture.
- Examples of open standards include X.509v3 Certificates, SSL/TLS, S/MIME, secured LDAP, and IPSec.

1.11. Maximum effectiveness and usability is ensured when security controls are located in the appropriate communication layer.

Rationale:

- Whenever security is required, the location in a communications protocol will have an impact. The impact may be on performance, reliance on an underlying network protocol, and on developers. Choosing the appropriate OSI layer in a communications protocol will maximize usability and minimize future changes.
- Security services can have an impact on performance. The impact is minimized when security services are located at lower layers of a communications protocol.
- Security services can have an impact on developers. For example, services provided at the transport layer have less impact on application programmers than services that run above that layer.
- Security services can increase reliance on a network protocol. An appropriate choice depends on the communication requirements of the business system.

1.12. Formalized trust agreements between Agencies and/or external entities establish the criteria for conducting business securely.

Rationale:

- The security posture of external entities should be carefully evaluated prior to establishing network communications to conduct business-oriented transactions or processes.
- Agreed upon minimum security standards must be verified by each entity annually.
- Even after trusted communications are allowed, most often these communications occur via a dedicated circuit or VPN into a tightly controlled area of the network, which then relays the information into other portions of the internal network for further processing.

1.13. Systems are resilient to threats, vulnerabilities, and cyber attacks[4] from both internal and external sources when properly designed and implemented.

Rationale:

- Zero-day vulnerabilities and Distributed Denial of Services attacks can occur at any time. Networks and systems must be designed such that operations can continue at acceptable levels.
- Government entities are primary targets for cyber attacks and cyber warfare.
- It is critical that the necessary actions are taken to protect information assets from internal as well as external attacks. Attacks or unauthorized access to information by employees can be very damaging, since they are more knowledgeable of the internal workings of an entity. Separation of duties and rotation of responsibilities can be used to protect against these types of attacks. Unannounced external third party reviews by security professionals are also very effective.

1.14. Obtaining superior levels of information assurance within State government depends on the use of properly trained security professionals[5].

Rationale:

- The expertise level of hackers is ever increasing. In addition hacking tools are widely available. Therefore, even novice hackers can cause significant damage to IT resources with very little effort. In many cases these types of attack have tended to be disruptive in nature, however, there is a second generation of hackers emerging that are focused on releasing destructive viruses and worms, or stealing monetary funds from e-commerce systems.
- Without the proper expertise and training, security implementations can be faulty and ineffective.

2. Technical Topic: Identification and Authentication

2.1. Practices:

2.1.1. Establish and follow industry accepted user-id & password management practices.

Rationale:

- User-ids & passwords are the most common means, but weakest form, of identification and authentication to State services. When not managed properly, unauthorized access is possible.

[4] NIST Special Publication 800-27 – Engineering Principles for Information Technology Security.

[5] NIST Special Publication 800-27 – Engineering Principles for Information Technology Security.

- User-ids and passwords must be carefully administered to ensure proper management (selection, aging, retirement, etc.) occurs.
- Examples of good management practices include requiring that passwords consist of upper and lower case characters, special characters, and numerics, which are at least 8 characters in length; required password change on a regular basis (e.g. monthly); required password rotation; disabling user-ids after three to five failed access attempts; not sharing user-ids and passwords with others; and not writing down passwords and hiding them in places that can be easily accessed.

2.1.2. Use vendor neutral, standards-based, APIs for identification and authentication.

Rationale:

- Avoid proprietary identification and authorization APIs, which promote vendor lock-in.
- Examples include NIST 800-63, Office of Budget and Management memoranda M-04-04, and GSA E-Authentication Technical Architecture standards.

2.1.3. Encrypt user-ids and passwords during transmission. In addition, passwords must be stored in an encrypted or one-way hash format.

Rationale:

- User-ids and passwords are the weakest method of identification and authentication. Transmitting or storing this information in the clear places the associated systems or data at great risk of unauthorized access.
- User-ids and passwords are easily captured when transmitted over IP networks.
- Legacy applications, that transmit passwords in the clear when encapsulated over IP networks, must also be securely transmitted.
- Security protocols such as SSL and IPSec and security solutions such as VPNs can be used to protect passwords in transit over networks.

2.1.4. Perform a risk management and cost benefit analysis before deciding to utilize biometrics for authentication.

Rationale:

- Biometrics as an authentication tool can be relatively expensive and complex to manage.
- Evaluating the risk vs. cost of implementing a new technology in lieu of existing security solutions should be carefully weighed.
- Biometrics techniques may vary in success in a real environment. Testing under real conditions may be necessary to determine effectiveness.
- Application integration with biometrics is hampered by a lack of standard APIs.
- Biometrics authentication complement and can be integrated with other security techniques such as digital signatures, smart cards and encryption.

2.1.5. Authenticate users prior to accessing controlled services or data.

Rationale:

- Allowing only authenticated users to access system resources protects those resources from inappropriate access.
- Authenticating users is the basis for providing accountability while permitting access.

2.1.6. Perform two-factor authentication when strong authentication is required.

Rationale:

- There are three accepted factors of authentication. The factors are “something you know” (e.g. password, passphrase, or PIN), “something you have” (e.g. token or smart card), and “something you are” (e.g. fingerprint, retina scan, or hand geometry).
- The authenticating factors listed above are a means of proving your stated identity. Strong authentication is accomplished when any two of these factors are provided during the authentication process.

2.1.7. Public Key Infrastructure (PKI) initiatives must interoperate with other PKI solutions, utilize a statewide approach, and conform to any relevant State law or statewide policy.

Rationale:

- The establishment of any PKI infrastructure is complex and must only be pursued after proper analysis and approvals have occurred. Agencies must leverage statewide services if they exist.
- Collaboration and co-operation will be required to support security services across the enterprise.
- A unified approach to a Public Key infrastructure enables the state to respond to changing requirements and conditions.
- A fragmented approach to a public key infrastructure will complicate administration and management of security across the enterprise.

2.1.8. Use industry accepted products for applications requiring digital certificate authentication.

Rationale:

- Certificates for web-based applications are provided by a number of major vendors. This approach is less risky and more cost effective than internal creation of digital certificates.
- Use of proprietary certificate extensions must be avoided to ensure interoperability.

2.1.9. PKI initiatives must store accurate system date and time.

- Rationale: The validity of digital signatures and electronic transactions depends on precise, reliable date and time information.
- Refer to the Platform Domain for further information regarding the time synchronization services.

2.2. Standards:

2.2.1. Use State Bureau of Investigation standards for live scan fingerprint capture and transmission.

Rationale:

- The State Bureau of Investigation (SBI) of the North Carolina Department of Justice has standards based on Federal Bureau of Investigation and ANSI/NIST fingerprint standards.

- These standards define a range of requirements for the electronic capture and transmission of fingerprint related data. Refer to the SAFIS Electronic Fingerprint Interface Specification (EFIS) for requirements related to fingerprints as an identification technique.
- Refer to the North Carolina CJIN website for specific references to the Statewide AFIS (SAFIS) and SAFIS EFIS standards.

2.2.2. Follow ISO/IEC 7811 standards for magnetic stripe cards.

Rationale:

- ISO 7811 defines the industry standards for magnetic stripe cards.

2.2.3. Follow ISO/IEC 7816 standards for contact smart cards.

Rationale:

- ISO 7816/1-4 standards define the electrical resistance, positioning of electrical contacts, communication protocol between card and card reader, and command set recognized by smart cards.
- They correspond roughly to the OSI layered model.
- The command set defined by the ISO 7816-4 standard are included in whole or in part by most smart cards on the market.

2.2.4. Follow ISO/IEC 14443 and NIST Government Smart Card Interoperability Specification V2.1 standards for contactless smart cards.

Rationale:

- ISO 14443 standards for contactless smart cards define the characteristics and communication protocols between contactless cards and the card reader.
- The Mifare architecture is the de facto global interface standard for contactless smart cards and is based on ISO 14443.

2.2.5. Follow PKCS #11 or PC/SC standards to interface smart cards to smart card readers.

Rationale:

- PKCS #11 from RSA is a widely accepted standard for integrating smart cards to applications supported by many vendors.
- PC/SC is widely accepted for integration of smart cards on Intel platforms.

2.2.6. Follow the BioAPI when interfacing applications and biometric information other than fingerprint biometrics (e.g. voice, face, iris, etc.).

Rationale:

- A consortium of vendors, technology developers, researchers, VARs, and end-users developed the BioAPI.
- The BioAPI offers interoperability over distributed environments with related APIs.
- They include SAPI, HA-API, the telecom industry’s S100 (a standard architecture for developing computer-telephony applications), and JavaSpeech (a standard for speech recognition using Java).
- Fingerprint biometrics must utilize standards specified by the NC SBI.
- Refer to the BioAPI Consortium for specific references to the BioAPI standards.

2.2.7. Follow the X.509v3 standard for Public Key Certificates.

Rationale:

- Public Key authentication must be based on Public Key Certificates.
- Public Key Certificates must be based on the X.509v3 standard.
- Despite the widespread acceptance of this standard, care must be taken when dealing with vendors. Projects should require proof of interoperability with existing or proposed enterprise implementations using X.509v3 certificates. Proprietary extensions to certificates could inhibit interoperability and should be avoided.

3. Technical Topic: Authorization and Access Control

3.1. Practices:

3.1.1. Only authorized users and devices are allowed to access the State's assets.

Rationale:

- Unauthorized access or use of state property such as a network, infrastructure device, or service is a violation of state law.

3.1.2. Authorize users according to the principle of least privilege. Security controls must be established that verify this requirement is satisfied on a regular basis.

Rationale:

- Authorize users to the minimum set of resources appropriate to their role.
- Authorizing users on least privilege minimizes the impact of security violations.
- Authorizing users to a minimum set of resources necessary to their function makes it easier to establish accountability.
- Authorization levels must be checked at least annually. A check on a monthly or quarterly basis is recommended.

3.1.3. All portable devices such as laptops, PDAs, smartphones, portable storage devices, etc. must be scanned and cleaned of any viruses by up-to-date anti-virus software prior to connecting to the State's network.

Rationale:

- Employees, contractors, consultants, sales representatives, etc. can be exposed to viruses while not behind firewalls or protected by out-of-date anti-virus software. In many cases, this is how viruses are introduced into the internal network.

3.1.4. Remote access to the internal network over a public network must occur through a VPN.

Rationale:

- Accessing application services securely across public networks require encrypted communications.

- Mobile workers (users that access the network from unpredictable locations), telecommuters and remote workers (users that routinely or occasionally work from a specific location), contractors, consultants, and vendors can easily expose userids, passwords, sensitive data, etc. over public networks.
- VPN technology is not required for web-based applications (e.g. email and calendar) if the communications are secured via SSL.
- Refer to the Security Zoning Technical Topic for more information concerning secure access from public networks.

3.1.5. Remote access to the internal network must be properly authenticated.

Rationale:

- Remote access users must be minimally authenticated using proper userid and password management practices. Additionally, strong (i.e. two-factor) authentication can be implemented, using technologies such as tokens, to further secure the remote access.
- Direct dial-in connections to modems located in desktops provide back door access to the internal network. Agencies must provide secure solutions to mobile workers, telecommuters, remote workers, contractors, consultants, and vendors to avoid this situation.
- Management of dial-in services is simplified by utilizing or implementing a centralized managed service such as an Agency modem bank.
- Applications and file systems must be protected from unauthorized access.

3.1.6. Virtual Private Network (VPN) solutions must utilize either SSL or IPSec technology.

Rationale:

- VPN solutions must be either SSL or IPSec based. While SSL is an open standard and therefore preferred, there may be times where IPSec would be a better choice based on the function being performed. IPSec, while a more proprietary solution, is also a recognized de facto standard.
- IPSec is an extension to the IP communications protocol, designed to provide end-to-end confidentiality for packets traveling over the Internet.
- IPSec works with both the current version of IPv4 and the new IPv6 protocol.

3.1.7. Mitigate security vulnerabilities that exist within various TCP/IP protocols.

Rationale:

- IP uses various protocols to provide and manage services. Due to the increased security requirements related to using the Internet, many of these protocols have security weaknesses that can negatively impact the State’s network, especially when uncontrolled entry into the state’s systems and networks is allowed.
- Insecure and/or unauthorized network protocols must not be allowed to enter into the State’s network. If use of network protocols is required either internally or externally then it must be tightly controlled or proxied from the Transaction Zone. Examples of insecure and unauthorized network protocols include NetBIOS, ICMP, and SNMP.
- The use of IPX poses significant risks across the State’s WAN. For that reason, routing IPX across the State’s network is no longer acceptable.

3.1.8. Use encryption technologies to provide information assurance and recoverability.

Rationale:

- Sensitive information may be susceptible to unauthorized access or viewing unless protected by encryption technologies.
- Many applications and operating systems create temporary files, which allow access to encrypted and even unencrypted information. Use of Agency supported encryption technologies ensure that this type of exposure is avoided.
- Organizations must have the means to recover data encrypted by an employee after the employee leaves or when encryption keys are lost or stolen. Many products do not provide data recovery services. Data recovery techniques must be developed whenever data encryption is used.

3.1.9. Protect desktops, laptops, PDAs, smartphones, etc. that are used by mobile and remote workers through the use of personal firewalls (hardware and/or software), encryption software, anti-spyware, and anti-virus software.

Rationale:

- Remote Access and telecommuting are becoming more and more common and therefore the data located on the devices used during remote access must be protected.
- Hackers looking for easy targets frequently scan remote users. These hackers may commandeer home systems to launch attacks, to destroy data, or to obtain access to the user’s work network.
- Personal firewalls, desktop encryption, virus protection, anti-spyware, and anti-virus software are a means of protecting remote users. End-users must be adequately trained in the use of these products.
- Use of fully functional purchased software is recommended for this critical function. Shareware products are generally not intended for wide spread use by an Agency, and in many cases this may be in violation of the software license agreement.
- Centrally configured firewalls and desktop encryption simplify the remote user’s need to manage potentially confusing products.
- Some firewall/VPN products provide configuration and administration support for personal firewalls.

3.1.10. Secure transmission of sensitive data in both wired and wireless environments.

Rationale:

- Data in transit to and from the enterprise must be protected in compliance with legal requirements for confidentiality and privacy.
- Web-enabled applications must protect confidential or critical data from unauthorized access.
- Use secure server-to-server communication to protect confidential or critical data transmissions.
- Examples of sensitive data include SSN, Credit Card numbers, health related information, etc.

- Examples of security protocols include SSL, VPN, Secure FTP, and WiFi Protected Access 2 (WPA2).

3.1.11. Use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) when secure communications between the web client and server is required.

Rationale:

- SSL/TLS is the most commonly supported protocol for communication between a Web Server and a browser.
- SSL/TLS authenticates the Web Server and optionally authenticates the user.
- Current implementations allow for client authentication support using the services provided by Certificate Authorities.

3.1.12. Cryptography must be based on open standards and utilize a key of sufficient length to adequately protect data.

Rationale:

- Cryptosystems and their associated cryptographic algorithms must be publicly reviewed and accepted by the security industry prior to any production usage, otherwise the validity and strength of the cryptosystem **cannot** be considered as a viable solution.
- The key lengths for these algorithms can vary; therefore the selection of an appropriate key size is critical to adequately protect data. In other words, select a key length large enough to ensure that the "work factor" (i.e. time and effort) required to defeat the protection is greater than the value of the "protected secret".
- The Cryptography Categories and Standards Table highlights open, industry accepted, cryptographic standards.

Cryptography Categories	Cryptography Algorithm Standards
Symmetric ("Shared" Secret Key)	AES, DES, 3DES, IDEA, RC4, RC5, RC6, Blowfish, Twofish
Asymmetric (Public Key / Private Key)	RSA, ECC, Diffie-Hellman, El Gamal, DSA
Hash Functions	MD5, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512

Table 1 - Cryptography Categories and Standards

3.1.13. Use S/MIME for securing email communications.

Rationale:

- S/MIME provides a consistent way to send and receive secure email including MIME data.
- S/MIME defines a protocol for encryption services and digital signatures.
- Email clients and servers should be evaluated for interoperability and support of the S/MIME standard.

4. Technical Topic: Administration

4.1. Practices:

4.1.1. Plan for security when developing applications and networks.

Rationale:

- Security is difficult and very expensive to retrofit into applications, therefore include security risk assessments and mitigation planning early in the development life cycle.
- Management must understand and manage risks associated with delivery of services. This is best accomplished by assessing risks prior to design, development, and implementation.

4.1.2. Proactively identify and implement preventative measures to common security threats and vulnerabilities[6].

Rationale:

- Behavioral and signature based anti-virus solutions, as well as other types of security solutions, should be utilized to deal proactively with security threats.
- Security bulletins received from organizations such as CERT Coordination Center should be authenticated and acted on promptly (i.e. according to patch management policies and procedures) to limit exposures to zero-day viruses, worms, etc.

4.1.3. Centralize security access and control services.

Rationale:

- Staffs with security expertise are difficult to obtain, train, and keep current in a distributed environment with rapidly changing technology and threats.
- Identifying threats, troubleshooting failures, and keeping a security infrastructure current could result in redundant and expensive overhead.
- Complex security arrangements lead to administrative problems and lessen overall security.

4.1.4. Use role-based administration.

Rationale:

- Role-based administration and multiple security domains are easier to administer and maintain than user-based privileges and single enterprise security domains.

4.1.5. Use the North Carolina Identity Service (NCID) for provisioning and authentication.

Rationale:

- Application specific authentication and authorization requires significant administrative overhead to maintain across multiple applications.
- Centralized authentication and authorization infrastructure and processes simplify information sharing within agencies and across multiple agencies.
- Centralized authorization simplifies application development by reducing the complexity of application-level security.
- Security oriented functions are complex to develop. Therefore, to limit security vulnerabilities, implementations should only be developed by trained security professionals.

[6] NIST Special Publication 800-27 – Engineering Principles for Information Technology Security.

4.1.6. Establish change management processes and procedures to ensure that change itself does not introduce new security vulnerabilities.

Rationale:

- Change configuration boards can assess the potential impact of changes to an operational environment.
- Changes to the existing environment (e.g. firewall ACLs, network configurations, application code, etc) are very complex and subject to human error, which can compromise security implementations.
- Compliance audits are a means of ensuring security is not compromised over time.
- All changes should be tested prior to implementation into production.

4.1.7. Develop, document, and regularly test Incident Response procedures. These procedures must include notification to the ITS Information Security Office (ISO).

Rationale:

- Even the best security practices and technology can be compromised.
- Planning is essential in responding to security incidents to ensure the protection of valuable data, collecting evidence to be used in prosecution efforts, and in recovering from an incident.
- Statewide policy requires incident reporting to the ITS ISO. Capturing these types of metrics is critical in assisting the State in protecting its critical IT assets in the future.
- Refer to the Enterprise System Management Domain for further information regarding the Disaster Recovery and Business Continuity Program development.

4.1.8. Use anti-virus and anti-spyware software to protect all mission critical systems (e.g. desktops, laptops, PDAs, smartphones, web servers, application servers, database servers, etc).

Rationale:

- Viruses, worms, and trojan horses cause significant disruption and financial costs to agencies.
- Transmission of viruses, worms, and trojan horses has become extremely common, with new variants occurring frequently.
- Behavioral and signature based anti-virus solutions, as well as other types of security solutions, should be utilized to deal proactively and in multiple ways with new and ever changing security threats.
- Anti-virus software must be installed, running and kept current through automatic updates on all desktops, laptops and handhelds.
- Anti-virus scanning must occur at the network perimeter to minimize internal infections. This would include email gateway servers.

4.1.9. Product versions of security related technologies must be either N or at N-1 and must be kept up to date by applying the latest security patches.

Rationale:

- Technologies that are not kept current become very vulnerable to security exploits.
- The use of dated technologies introduces legacy support issues.

5. Technical Topic: Audit

5.1. Practices:

5.1.1. Audit logs for critical systems and functions must be well managed.

Rationale:

- Proper management of audit logs is essential in providing information assurance. Audit logs must be properly collected, protected, maintained, and archived to ensure that proactive analysis and forensic examination can occur as required.
- Due to the critical nature of audit logs, hackers often attempt to alter audit log information. For this reason, additional security controls should be taken to protect these security assets.
- To establish accountability a capability to track and monitor all relevant activity must be available.
- Detection of security violations requires the capability to track security relevant activity.

5.1.2. Audit logs must be monitored on a frequent and regular basis.

Rationale:

- In many cases audit logs can be used both proactively and reactively to minimize the effects of a security intrusion or incident.
- Daily review (automated and manual) of audit logs is essential in both understanding access control characteristics and identifying potential or actual security concerns.

5.1.3. Audit security processes as well as security implementations at least once a year.

Rationale:

- Defects in processes and procedures can nullify the effectiveness of implemented security solutions.
- Internal and external audits should include security policies and procedures.

5.1.4. Implement and actively monitor Host Intrusion Detection Systems (IDS) and Host Intrusion Prevention Systems (IPS) to protect mission-critical systems.

Rationale:

- Host detection and prevention systems should be placed on critical services to ensure tampering with critical applications can be detected and corrected.
- An attack on mission-critical systems can significantly impact the discharge of the state’s responsibilities.
- Automated tools simplify monitoring for security incidents.

5.1.5. Implement and actively monitor Network Intrusion Detection Systems (IDS) and Network Intrusion Prevention Systems (IPS) to protect networks.

Rationale:

- Network detection and prevention systems should be placed in areas of the network to facilitate monitoring and protecting critical networks (e.g. Transaction Zone, critical application sub-nets)
- Proper separation of duties should be implemented such that network and system administrators are not also responsible for IDS monitoring. If this is not possible, an impartial third party should perform unannounced external analysis to ensure that proper checks and balances are in place.

6. Technical Topic: Security Zoning

6.1. Practices:

6.1.1. All system components (e.g. servers, devices, desktops) must reside in the appropriate security zone and be secured as required by statewide policy.

Rationale:

- The Security Framework Policy establishes the minimum operational, management, and audit controls for various security zones.
- By locating resources (e.g. desktop, web server, application server, database server, etc.) in the appropriate security zones and placing the proper controls on the resources in those zones, Agency information assets become much more secure and much less vulnerable to attack.

6.1.2. Communications across Secure Zones must be denied by default unless explicitly allowed.

Rationale:

- In order to protect the increasing levels of trust in the security zone environment, communications from user to application or application-to-application must be strictly controlled.
- Following the industry best practice of “implicitly deny unless explicitly allowed” provides a high level of security assurance.

6.1.3. Utilize the State’s Enterprise Service Access Point (ESAP) and other infrastructure services to comply with statewide requirements.

Rationale:

- ITS offers enterprise-class infrastructure network and hosting services that provides many benefits such as economies of scale, 24x7x365 support, disaster recovery, etc. Agencies that utilize the State’s enterprise services will be able to protect their resources and comply with statewide requirements without having to deal with the day-to-day maintenance and support functions that are required to support this type of environment.
- Agencies may choose to create their own security zones; however, the cost of such an endeavor may be excessive. Any agency that opts for this approach must ensure that the required activities are being performed on an annual basis.
- Compliance with this standard practice is consistent with the principle of Defense-in-Depth.

6.1.4. Place Web Servers, FTP Servers, and other servers that need to be publicly accessed in a Demilitarized Zone (DMZ).

Rationale:

- Web, FTP, and other servers, which need to be accessed by the public, are highly susceptible to attack on the Internet, and must be located in an isolated area of the network.
- Placement of public servers on the internal network opens the network to uncontrolled anonymous traffic. This is dangerous to systems and networks.

6.1.5. Place Application Servers, Database Servers, Intranet Web Servers and other servers that must be privately accessed behind a firewall a Secure and/or Special Assemblies Zone.

Rationale:

- Application services must be protected from unwanted external access and must be proxied from the DMZ.
- All communication from servers in the DMZ to internal applications and services must comply with firewall rules.
- Usage of specific application protocols and ports can be tightly controlled via firewall access control lists across the zones.
- Placing servers in increasingly secure zones provides the ability to apply fine-grained security controls.

6.1.6. Place Desktops, Laptops, PDAs, Smartphones and other similar devices behind a firewall in a Secure and/or Special Assemblies Zone.

Rationale:

- Internal networks must always be behind a firewall’s private interface and utilize private addresses; otherwise these resources are easily accessible via the Internet.
- Remote access to the internal network must be properly authenticated and must occur through a VPN.
- Docking stations for devices such as PDA, smartphones, etc. must be located behind a firewall.

6.1.7. Place other infrastructure services (e.g. DNS, email, etc.) in the most Secure Zone and/or Special Assemblies Zone possible.

Rationale:

- The placement of some infrastructure services is often dependent on inter-related criteria; therefore services must be made as secure as possible, while still being able to perform its desired function.
- In most cases, the placement of an infrastructure related service will span several zones.
- Email relays should be placed in the DMZ to avoid direct access to internal email servers/message stores. Email servers/messages stores should be placed behind a firewall in the internal network.
- Domain Naming Services should be implemented as ‘split’ DNS. All external requests for naming services should only be directed to an external DNS server located in the Transaction Zone, which has a limited view of internal DNS data and contains all advertised services.